ESET NOD32 Antivirus 4

Business Edition para Linux Desktop

Manual de instalação e Guia do usuário

Clique aqui para fazer download da versão mais recente deste documento

ESET NOD32 Antivirus 4

Atendimento ao cliente mundial: www.eset.com/support

REV. 8.4.2011

Índice

1. ESET NOD32 Antivirus

Como resultado da popularidade cada vez maior dos sistemas operacionais baseados em Unix, os usuários de malwares estão desenvolvendo mais ameaças visando os usuários do Linux. O ESET NOD32 Antivirus oferece proteção poderosa e eficaz contra ameaças. O ESET NOD32 Antivirus inclui a capacidade de desviar ameaças do Windows, protegendo os usuários do Linux à medida que eles interagem com usuários do Windows e vice-versa. Apesar de os malwares do Windows não representarem uma ameaça direta ao Linux, a desativação dos malwares que infectaram uma máquina do Linux impedirá a sua expansão para computadores baseados em Windows, por meio de uma rede local ou da Internet.

1.1 Requisitos do sistema

Para uma operação sem interrupções do ESET NOD32 Antivirus, o sistema deve atender aos seguintes requisitos de hardware e de software:

ESET NOD32 Antivirus:

	Requisitos do sistema
Arquitetura do processador	32 bits, 64 bits AMD®, Intel®
Sistema	Distribuições baseadas em Debian e RedHat (Ubuntu, OpenSuse, Fedora, Mandriva, RedHat etc.) kernel 2.6.x GNU C Library 2.3 ou posterior GTK+ 2.6 ou posterior Compatibilidade recomendada de LSB 3.1
Memória	512 MB
Espaço livre em disco	100 MB

2. Instalação

Antes de iniciar o processo de instalação, feche todos os programas abertos no computador. O ESET NOD32 Antivirus contém componentes que podem entrar em conflito com outros programas antivírus que já podem estar instalados no computador. A ESET recomenda que você remova qualquer outro programa para evitar problemas potenciais. Você pode instalar o ESET NOD32 Antivirus a partir de um CD de instalação ou de um arquivo disponível no site da ESET.

Para iniciar o assistente de instalação, execute uma das seguintes ações:

- Se estiver instalando a partir do CD de instalação, insira o CD na unidade de CD-ROM. Clique duas vezes no ícone de instalação do ESET NOD32 Antivirus para iniciar o instalador.
- Se estiver instalando a partir de um arquivo obtido por download, clique com o botão direito do mouse e clique na guia **Propriedades > Permissões**, marque a opção **Permitir execução do arquivo como programa** e feche a janela. Clique duas vezes no arquivo para iniciar o instalador.

Inicie o instalador e o assistente de instalação o guiará pela configuração básica. Após concordar com o Contrato de licença de usuário final, você poderá escolher um dos seguintes tipos de instalação:

- Instalação típica 5
- Instalação personalizada 5
- Instalação remota 6

2.1 Instalação típica

A instalação típica inclui as opções de configuração apropriadas para a maioria dos usuários. As configurações proporcionam segurança máxima combinada com o excelente desempenho do sistema. A instalação típica é a opção padrão e é recomendada se você não possui requisitos particulares para configurações específicas.

Após selecionar o modo de instalação **Típica (recomendada)**, você será solicitado a digitar seu nome de usuário e senha para ativar as atualizações automáticas do programa. Essa etapa tem um papel significativo no fornecimento de proteção constante ao seu sistema. Insira o **Usuário** e a **Senha** (os dados de autenticação recebidos após a compra ou registro do produto) nos campos correspondentes. Caso não tenha o nome de usuário e a senha disponíveis no momento, você pode selecionar a opção **Configurar parâmetros de atualização mais tarde** para continuar a instalação.

O **ThreatSense.Net Early Warning System** ajuda a garantir que a ESET seja informada contínua e imediatamente sobre novas ameaças para proteger os clientes rapidamente. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar o ThreatSense.Net Early Warning System** é selecionada. Clique em **Configurar...** para modificar as configurações detalhadas para o envio de arquivos suspeitos. (Para obter mais informações, consulte ThreatSense.Net 20).

A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento. Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET NOD32 Antivirus detecte este tipo de ameaça (recomendável). Se não desejar ativar esse recurso, selecione a opção **Desativar detecção de aplicativos potencialmente não desejados**.

Clique em **Instalar** para concluir a instalação.

2.2 Instalação personalizada

A instalação personalizada é destinada a usuários experientes que desejam modificar as configurações avançadas durante o processo de instalação.

Após selecionar o modo de instalação **Personalizada**, você precisará digitar o seu **Nome de usuário** e a **Senha** (os dados de autenticação recebidos após a compra ou o registro de seu produto) nos campos correspondentes. Caso não tenha o nome de usuário e a senha disponíveis no momento, você pode selecionar a opção **Configurar parâmetros de atualização mais tarde** para continuar a instalação. Você precisará digitar o seu usuário e a sua senha posteriormente.

Se estiver utilizando um servidor proxy, você poderá definir os parâmetros agora, selecionando a opção **Eu utilizo um servidor proxy**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **usuário** e uma **senha** válidos a fim de obter acesso ao servidor proxy. Se tiver certeza de que nenhum servidor proxy está sendo utilizado, escolha a opção **Eu não utilizo um servidor proxy**.

Se o ESET NOD32 Antivirus for administrado pelo ESET Remote Administrator (ERA), você poderá definir os parâmetros do ERA Server (nome do servidor, porta e senha) para conectar automaticamente o ESET NOD32 Antivirus ao ERA Server após a instalação.

Na próxima etapa, você poderá **Definir usuários privilegiados** que poderão editar a configuração do programa. Em uma lista de usuários, no lado esquerdo, selecione os usuários e selecione **Adicionar** para incluí-los na lista **Usuários privilegiados**. Para exibir todos os usuários do sistema, selecione a opção **Mostrar todos os usuários**.

O **ThreatSense.Net Early Warning System** ajuda a garantir que a ESET seja informada contínua e imediatamente sobre novas ameaças para proteger os clientes rapidamente. O sistema permite o envio de novas ameaças para o Laboratório de

ameaças da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar o ThreatSense.Net Early Warning System** é selecionada. Clique em **Configurar...** para modificar as configurações detalhadas para o envio de arquivos suspeitos. Para obter mais informações, consulte ThreatSense.Net 20.

A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento. Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET NOD32 Antivirus detecte este tipo de ameaça (recomendável).

Clique em **Instalar** para concluir a instalação.

2.3 Instalação remota

A instalação remota permite que você crie um pacote de instalação (arquivo de instalação *.linux*) que pode ser instalado em computadores de destino. Com isso é possível gerenciar o ESET NOD32 Antivirus remotamente por meio do ESET Remote Administrator.

Após selecionar o modo de instalação remota (opção **Preparar** ESET NOD32 Antivirus **para instalação remota**), será exibida a solicitação para que você digite o seu nome de usuário e a sua senha para ativar as atualizações automáticas do ESET NOD32 Antivirus. Insira o **Usuário** e a **Senha** (os dados de autenticação recebidos após a compra ou registro do produto) nos campos correspondentes. Caso não tenha o nome de usuário e a senha disponíveis no momento, você pode selecionar a opção **Configurar parâmetros de atualização mais tarde** para continuar a instalação. Posteriormente você poderá digitar o seu nome de usuário e a sua senha diretamente no programa.

A próxima etapa será a configuração da sua conexão com a Internet. Se estiver utilizando um servidor proxy, você poderá definir os parâmetros agora, selecionando a opção **Eu utilizo um servidor proxy**. Se tiver certeza de que nenhum servidor proxy está sendo utilizado, você poderá escolher a opção **Eu não utilizo um servidor proxy**.

Na etapa seguinte, defina os parâmetros do ERA Server para conectar automaticamente o ESET NOD32 Antivirus ao ERA Server após a instalação. Para ativar a administração remota, selecione a opção **Conectar ao servidor de Administração Remota**. O **Intervalo de conexões do servidor** designa a frequência com que o ESET NOD32 Antivirus conectará ao ERA Server. No campo **Remote Administrator Server**, especifique o endereço do servidor (onde o ERA Server é instalado) e o número da porta. Esse campo contém uma porta de servidor predefinida, que é utilizada para a conexão de rede. Recomendamos que você deixe a configuração de porta padrão em *2222*. Se a conexão com o ERA Server estiver protegida por uma senha, marque **O servidor do Remote Administrator requer autenticação** e digite a senha no campo **Senha**. Normalmente, somente o servidor **Primário** precisa ser configurado. Se estiver executando diversos servidores ERA na rede, é possível optar por adicionar outra conexão do ERA Server **Secundário**. Servirá como a solução de fallback. Se o servidor primário ficar inacessível, o ESET NOD32 Antivirus entrará em contato automaticamente com o ERA Server secundário. O ESET NOD32 Antivirus também tentará restabelecer a conexão com o servidor primário. Depois que essa conexão estiver ativa novamente, o ESET NOD32 Antivirus retornará ao servidor primário. A configuração de dois perfis de servidores de administração remota é mais bem utilizada por clientes móveis com notebooks que se conectam à rede local e fora da rede.

Na próxima etapa, você poderá **Definir usuários privilegiados** que poderão editar a configuração do programa. Em uma lista de usuários, no lado esquerdo, selecione os usuários e selecione **Adicionar** para incluí-los na lista **Usuários privilegiados**. Para exibir todos os usuários do sistema, selecione a opção **Mostrar todos os usuários**.

O **ThreatSense.Net Early Warning System** ajuda a garantir que a ESET seja informada contínua e imediatamente sobre novas ameaças para proteger os clientes rapidamente. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar o ThreatSense.Net Early Warning System** é selecionada. Clique em **Configurar...** para modificar as configurações detalhadas para o envio de arquivos suspeitos. Para obter mais informações, consulte ThreatSense.Net 20.

A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento. Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET NOD32 Antivirus detecte este tipo de ameaça (recomendável).

Na última etapa do assistente de instalação, escolha uma pasta de destino. O instalador da ESET criará o arquivo de instalação *.linux*.

Este arquivo pode ser instalado em computadores remotos que utilizam o protocolo de rede Shell Seguro (SSH) ou Cópia Segura (SCP). Abra o Terminal e digite um comando no seguinte formato:

```
scp SourceFile user@host:/target
```

Exemplo:

```
scp ueavbe.i386.en.00.linux
administrator@100.100.1.1:/home/administrator
```

Para obter mais informações sobre como utilizar a Cópia segura, digite o comando `man scp` no Terminal.

2.4 Inserção do usuário e da senha

Para obter a funcionalidade ideal, é importante configurar o programa para que ele faça o download automático de atualizações do banco de dados de assinatura de vírus. Isso somente será possível se o **Usuário** e a **Senha** corretos forem digitados na Configuração da atualização 16.

2.5 Rastreamento sob demanda do computador

Após instalar o ESET NOD32 Antivirus, deverá ser executado um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, em **Rastreamento inteligente**. Para obter mais informações sobre os rastreamentos sob demanda do computador, consulte a seção Rastreamento sob demanda do computador 11.

3. Guia para iniciantes

Este capítulo fornece uma visão geral inicial do ESET NOD32 Antivirus e de suas configurações básicas.

3.1 Introdução ao design da interface do usuário - modos

A janela principal do ESET NOD32 Antivirus é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

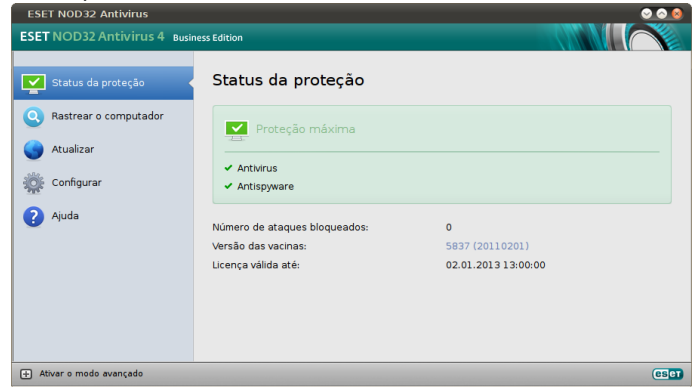
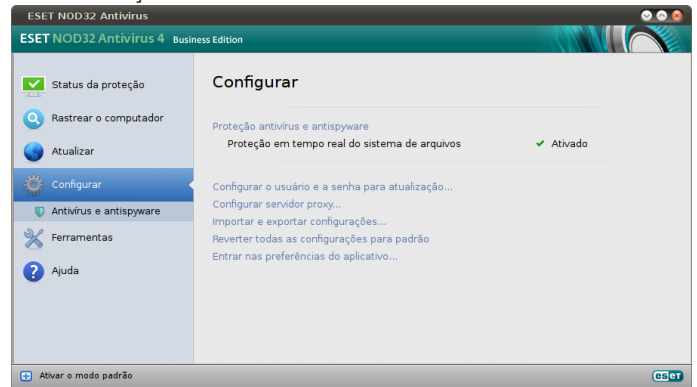
- **Status da proteção** - Fornece informações sobre o status da proteção do ESET NOD32 Antivirus. Se o **Modo avançado** estiver ativado, o submenu **Estatísticas** será exibido.
- **Rastrear o computador** - Essa opção permite que você configure e inicie o **Rastreamento sob demanda do computador**.
- **Atualizar** - Exibe informações sobre as atualizações do banco de dados de assinatura de vírus.
- **Configuração** - Selecione essa opção para ajustar o nível de segurança do seu computador. Se o **Modo avançado** estiver ativado, o submenu **Antivírus e antispyware** será exibido.
- **Ferramentas** - Fornece o acesso a **Relatórios**, **Quarentena** e **Agenda**. Essa opção é exibida somente no **Modo avançado**.
- **Ajuda** - Fornece informações sobre o programa, acesso a arquivos de ajuda, à base de dados de conhecimento da Internet e ao site da ESET.

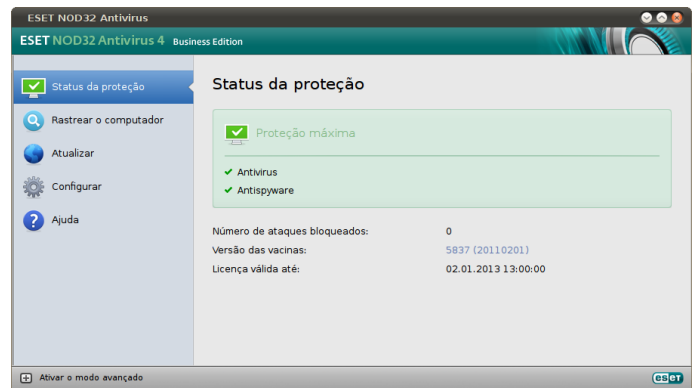
A interface do usuário do ESET NOD32 Antivirus permite que os usuários alternem entre o Modo padrão e avançado. O modo padrão fornece acesso aos recursos necessários para operações comuns. Ele não exibe opções avançadas. Para alternar entre os modos, clique no ícone de adição (**+**), próximo a **Ativar o modo avançado/Ativar o modo padrão**, no canto inferior esquerdo da janela principal do programa.

O Modo padrão fornece acesso aos recursos necessários para operações comuns. Ele não exibe opções avançadas.

A alternância para o modo Avançado adiciona a opção **Ferramentas** ao menu principal. A opção **Ferramentas** permite que você acesse os submenus **Relatórios**, **Quarentena** e **Agenda**.

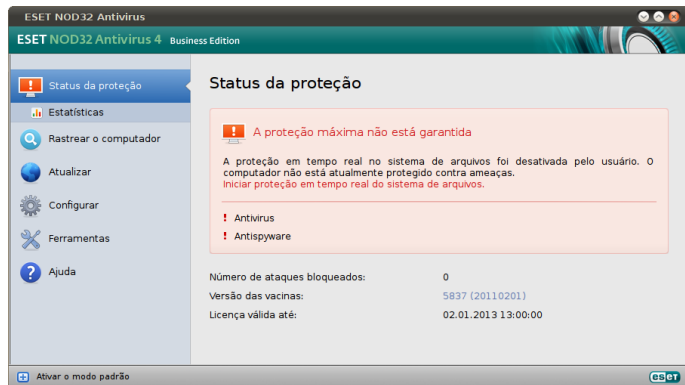
OBSERVAÇÃO: Todas as instruções restantes deste guia ocorrem no **Modo avançado**.

Modo padrão:

Modo avançado:

3.1.1 Verificação do funcionamento do sistema

Para exibir o **Status da proteção**, clique na opção superior do menu principal. Um resumo de status sobre o funcionamento do ESET NOD32 Antivirus será exibido na janela primária e também no submenu com **Estatísticas**. Selecione-o para exibir as informações mais detalhadas e as estatísticas sobre os rastreamentos do computador que foram realizados no sistema. A janela Estatísticas está disponível somente no modo avançado.

3.1.2 O que fazer se o programa não funcionar adequadamente

Se os módulos ativados estiverem funcionando adequadamente, um ícone de marcação verde será atribuído a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido, e informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status dos módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda** para acessar os arquivos de ajuda ou pesquisar na base de dados de conhecimento.

Se precisar de assistência, entre em contato com o Atendimento ao cliente da ESET no site da ESET. O Atendimento ao cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a determinar uma resolução.

4. Trabalhar com ESET NOD32 Antivirus

4.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos, modificando arquivos que representam ameaças internas. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

4.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

4.1.1.1 Configuração da proteção em tempo real

A proteção do sistema de arquivos em tempo real verifica todos os tipos de mídia, e o rastreamento é disparado por vários eventos. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção denominada Configuração de parâmetros do mecanismo ThreatSense 13), a proteção do sistema de arquivos em tempo real pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Por padrão, a proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outro rastreador em tempo real), a proteção em tempo real pode ser terminada, clicando no ícone do ESET NOD32 Antivirus localizado na barra de menus (topo da tela) e selecionando a opção **Desativar a proteção em tempo real do sistema de arquivos**. A proteção em tempo real também pode ser terminada na janela principal do programa (**Configurar** > **Antivírus e antispyware** > **Desativar**).

Para modificar as configurações avançadas da proteção em tempo real, vá para **Configuração** > **Entrar nas preferências do aplicativo...** > **Proteção** > **Proteção em tempo real** e clique no botão **Configurar...**, próximo das **Opções avançadas** (descritas na seção denominada Opções de rastreamento avançadas 10).

4.1.1.1.1 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são rastreados na **abertura**, **criação** ou **execução**. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

4.1.1.1.2 Opções de rastreamento avançadas

Nessa janela, é possível definir os tipos de objeto que serão rastreados pelo mecanismo ThreatSense, ativar/desativar **Heurística avançada** e também modificar as configurações de arquivos compactados e cache de arquivo.

Não recomendamos alterar os valores padrão na seção **Configurações padrão de arquivos compactados**, a menos que seja necessário resolver um problema específico, pois os valores maiores de compactação de arquivos compactados podem impedir o desempenho do sistema.

Você pode alternar o rastreamento da Heurística avançada do ThreatSense para arquivos executados e também para arquivos criados e modificados separadamente, clicando na caixa de seleção **Heurística avançada** em cada uma das respectivas seções de parâmetros do ThreatSense.

Para proporcionar o impacto mínimo no sistema ao usar a proteção em tempo real, você pode definir o tamanho do cache de otimização. Esse comportamento fica ativo durante a utilização da opção **Ativar cache de arquivo limpo**. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Os arquivos não serão rastreados repetidamente após serem ocultados (a menos que sejam modificados), até o tamanho definido do cache. Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus.

Clique em **Ativar cache de arquivo limpo** para ativar/desativar essa função. Para definir a quantidade de arquivos que serão ocultados, basta digitar o valor desejado no campo de entrada, ao lado de **Tamanho do cache**.

Os parâmetros de rastreamento adicionais podem ser configurados na janela **Configuração do mecanismo ThreatSense**. Você pode definir os tipos de **Objetos** que devem ser rastreados, utilizando o nível **Opções** e **Limpeza** e também definindo **Extensões** e **Limites** de tamanho de arquivos para a proteção em tempo real do sistema de arquivos. Você pode inserir a janela de configuração do mecanismo ThreatSense, clicando no botão **Configurar...** ao lado de**Mecanismo ThreatSense**, na janela Configuração avançada. Para obter informações mais detalhadas sobre os parâmetros do mecanismo ThreatSense, consulte Configuração de parâmetros do mecanismo ThreatSense 13.

4.1.1.1.3 Exclusões do rastreamento

Esta seção permite que você exclua determinados arquivos e pastas do rastreamento.

- **Caminho** - caminho para arquivos e pastas excluídos
- **Ameaça** - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, e não completamente. Portanto, se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus.

- **Adicionar...** - exclui objetos da detecção. Insira o caminho para um objeto (você também pode utilizar caracteres curinga *e ?) ou selecione a pasta ou o arquivo na estrutura em árvore.
- **Editar...** - permite que você edite as entradas selecionadas.
- **Remover** - remove as entradas selecionadas.
- **Padrão** - cancela todas as exclusões.

4.1.1.2 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Tenha cautela ao modificar os parâmetros da proteção em tempo real. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver uma situação de conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

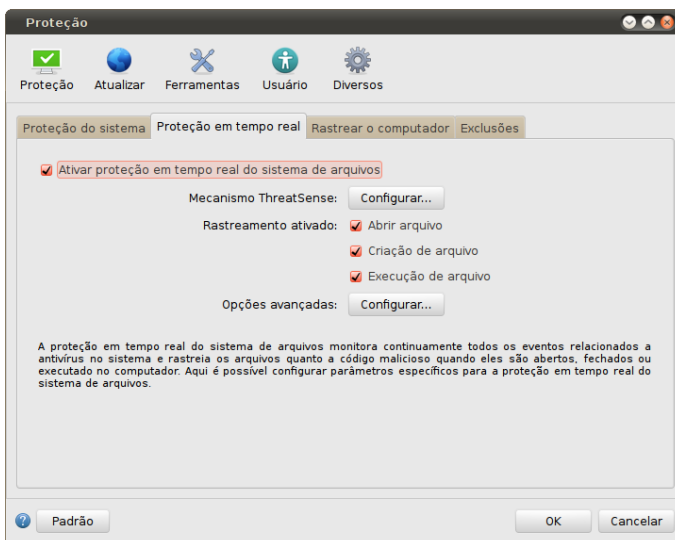
Após a instalação do ESET NOD32 Antivirus, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior esquerda da janela **Proteção em tempo real** (**Configuração** > **Entrar nas preferências do aplicativo ...** > **Proteção** > **Proteção em tempo real**).

4.1.1.3 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, utilize o arquivo de teste eicar.com. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pelo instituto EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

4.1.1.4 O que fazer se a proteção em tempo real não funcionar

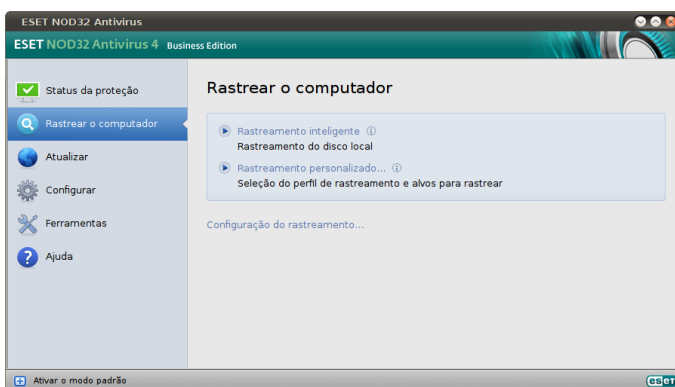
Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada
Se a proteção em tempo real foi inadvertidamente desativada por um usuário, será preciso reativá-la. Para reativar a Proteção em tempo real, navegue até **Configuração** > **Antivírus e antispyware** e clique no link **Ativar proteção em tempo real do sistema de arquivos** (à direita) na janela principal do programa. Como alternativa, você pode ativar a proteção em tempo real do sistema de arquivos na janela Configuração avançada, em **Proteção** > **Proteção em tempo real**, selecionando a opção **Ativar proteção em tempo real do sistema de arquivos**.

Proteção em tempo real não detecta nem limpa infiltrações
Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas poderão entrar em conflito. Recomendamos desinstalar outros programas antivírus que possam estar no sistema.

Proteção em tempo real não é iniciada
Se a proteção em tempo real não for ativada na inicialização do sistema, talvez haja conflitos com outros programas. Se for este o caso, consulte os especialistas do Atendimento ao cliente da ESET.

4.1.2 Rastreamento sob demanda do computador

Caso suspeite que seu computador esteja infectado (se ele se comportar de maneira anormal), execute **Rastreamento do computador** > **Rastreamento inteligente** para examinar se há ameaças no computador. Para obter proteção máxima, os rastreamentos do computador devem ser executados regularmente como parte das medidas usuais de segurança; não faça rastreamentos somente sob suspeita de infecção. O rastreamento normal pode detectar infiltrações que não foram detectadas pelo rastreador em tempo real quando foram salvas no disco. Isso pode acontecer caso o rastreador em tempo real esteja desativado no momento da infecção ou se o banco de dados de assinatura de vírus não estiver atualizado.

Recomendamos que execute um Rastreamento sob demanda do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

4.1.2.1 Tipos de rastreamento

Há dois tipos de rastreamento sob demanda do computador disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

4.1.2.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. Suas principais vantagens são a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento inteligente verifica todos os arquivos em todas as pastas e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a seção sobre Limpeza 14.

4.1.2.1.2 Rastreamento personalizado

O **Rastreamento personalizado** é excelente caso deseje especificar parâmetros de rastreamento, como alvos de rastreamento e métodos de rastreamento. A vantagem de executar o Rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. Diferentes configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastrear o computador** > **Rastreamento personalizado** e selecione **Alvos de rastreamento** na estrutura em árvore. Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**.

A realização de rastreamentos de computador com o Rastreamento personalizado é recomendada para usuários avançados com experiência anterior na utilização de programas antivírus.

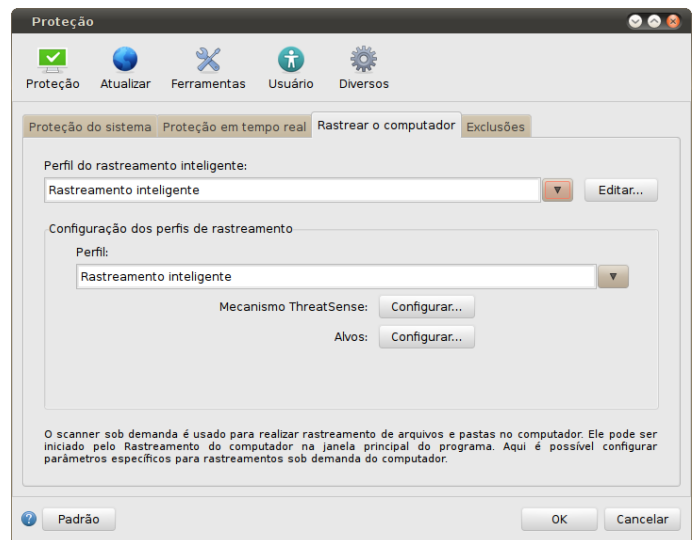
4.1.2.2 Alvos de rastreamento

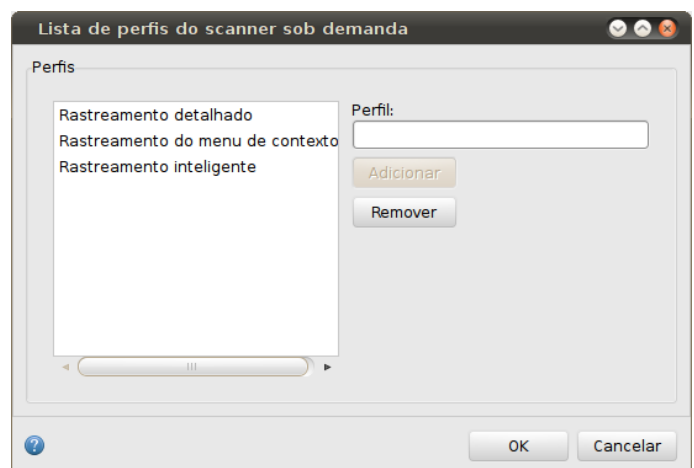
A estrutura em árvore de Alvos de rastreamento permite que você selecione arquivos e pastas que serão rastreados em busca de vírus. As pastas também podem ser selecionadas de acordo com as configurações de um perfil.

Um alvo de rastreamento pode ser mais exatamente definido por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore que lista todas as pastas disponíveis no computador.

4.1.2.3 Perfis de rastreamento

As suas configurações de rastreamento favoritas podem ser salvas para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, vá para **Configuração** > **Entrar nas preferências do aplicativo ...** > **Proteção** > **Rastreamento do computador** e clique em **Editar...** ao lado da lista de perfis atuais.

Para ajudar a criar um perfil de rastreamento a fim de atender às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense 13 para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a Limpeza rígida. Na janela **Lista de perfis do scanner sob demanda**, escreva o nome do perfil, clique no botão **Adicionar** e confirme clicando em **OK**. Ajuste os parâmetros que atendam aos seus requisitos, configurando o **Mecanismo ThreatSense** e **Alvos de rastreamento**.

4.1.3 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é o nome da tecnologia que consiste em métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para entrar na janela de configuração, clique em **Configuração** > **Antivírus e antispyware** > **Configuração avançada da proteção antivírus e antispyware** e clique no botão **Configurar...** , localizado nos caracteres curinga **Proteção do sistema**, **Proteção em tempo real** e **Rastrear o computador** que utilizam a tecnologia ThreatSense (veja abaixo). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- **Proteção do sistema** > Rastreamento de arquivo na inicialização do sistema
- **Proteção em tempo real** > Proteção em tempo real do sistema de arquivos
- **Rastrear o computador** > Rastreamento sob demanda do computador

Os parâmetros do ThreatSense são especialmente otimizados para cada módulo e a modificação deles pode influenciar significativamente o funcionamento do sistema. Por exemplo, a alteração das configurações para sempre rastrear empacotadores em tempo real ou a ativação da heurística avançada no módulo de proteção em tempo real de sistema de arquivos podem resultar em um sistema mais lento. Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastrear o computador.

4.1.3.1 Objetos

A seção **Objetos** permite definir quais arquivos do computador serão rastreados quanto a infiltrações.

- **Arquivos** - fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de banco de dados etc.)
- **Links simbólicos** - (somente scanner sob demanda) rastreia determinados tipos especiais de arquivos que contenham uma cadeia de caracteres de texto que seja interpretada e seguida pelo sistema operacional como um caminho para outro arquivo ou diretório.
- **Arquivos de email** - (não disponível na Proteção em tempo real) rastreia arquivos especiais que contenham mensagens de e-mail.
- **Caixas de correio** - (não disponível na Proteção em tempo real) rastreia as caixas de correio do usuário no sistema. A utilização incorreta dessa opção pode resultar em um conflito com o seu cliente de e-mail. Para saber mais sobre as vantagens e desvantagens dessa opção, leia o seguinte artigo da base de dados de conhecimento.
- **Arquivos compactados** - (não disponível na proteção em tempo real) fornece o rastreamento de arquivos compactados (.rar, .zip, .arj, .tar, etc.).
- **Arquivos compactados de auto-extração** - (não disponível na Proteção em tempo real) rastreia arquivos contidos em arquivos compactados de auto-extração.
- **Empacotadores em tempo real** - diferente dos tipos de arquivos compactados padrão, os empacotadores em tempo real são descompactados na memória, além de empacotadores estáticos padrão (UPX, yoda, ASPack, FGS etc.).

4.1.3.2 Opções

Na seção **Opções**, você pode selecionar os métodos utilizados durante um rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

- **Banco de dados de assinatura de vírus** - As assinaturas podem detectar e identificar ameaças pelo nome, com exatidão e confiabilidade, usando o banco de dados de assinatura de vírus.
- **Heurística** - A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).
- **Heurística avançada** - A heurística avançada é formada por um algoritmo heurístico exclusivo, desenvolvido pela ESET e otimizado para a detecção de worms e cavalos de troia de computador escritos em linguagens de programação de alto nível. A capacidade de detecção do programa é significativamente maior por causa da heurística avançada.
- **Adware/Spyware/Riskware** - Esta categoria inclui o software que coleta informações confidenciais sobre usuários sem o consentimento informado deles. E inclui também software que exibe material de propaganda.

- **Aplicativos potencialmente indesejados** - Esses aplicativos não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de maneira negativa. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao modo anterior à instalação desses aplicativos). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.
- **Aplicativos potencialmente inseguros** - esses aplicativos referem-se a softwares comerciais e legítimos que podem sofrer abusos por parte de invasores, caso tenham sido instalados sem o conhecimento do usuário. Essa classificação inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

4.1.3.3 Limpeza

As configurações de limpeza determinam como o scanner limpa os arquivos infectados. Há três níveis de limpeza:

- **Sem limpeza** - Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que você escolha uma ação.
- **Limpeza padrão** O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a serem seguidas. A escolha das ações a serem seguidas também será exibida se uma ação predefinida não for completada.
- **Limpeza rígida** O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos compactados). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, será oferecida a você uma ação a ser tomada na janela de aviso.

Aviso: No modo de limpeza Padrão, o arquivo compactado inteiro será excluído somente se todos os arquivos do arquivo compactado estiverem infectados. Se no arquivo compactado houver arquivos legítimos, ele não será excluído. Se um arquivo do arquivo compactado infectado for detectado no modo de Limpeza rígida, todo o arquivo compactado será excluído, mesmo se houver arquivos limpos.

4.1.3.4 Extensões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Esta seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem excluídos do rastreamento.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Com os botões **Adicionar** e **Remover**, você pode habilitar ou proibir o rastreamento das extensões desejadas.

A exclusão de arquivos do rastreamento será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento adequado de um programa que está utilizando as extensões. Por exemplo, pode ser aconselhável excluir as extensões *.log*, *.cfg* e *.tmp*.

4.1.3.5 Limites

A seção **Limites** permite especificar o tamanho máximo de objetos e os níveis de compactação de arquivos compactados a serem rastreados:

- **Tamanho máximo:**Define o tamanho máximo dos objetos que serão rastreados. O módulo antivírus rastreará apenas objetos menores que o tamanho especificado. Não recomendamos alterar o valor padrão, pois geralmente não há razão para modificá-lo. Essa opção deverá ser alterada apenas por usuários avançados que tenham razões específicas para excluir objetos maiores do rastreamento.
- **Tempo máximo do rastreamento:**Define o tempo máximo designado para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento.
- **Nível de compactação de arquivos:**Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá desmarcado.
- **Tamanho máximo do arquivo:** Esta opção permite especificar o tamanho máximo de arquivo dos arquivos contidos em arquivos compactados (quando são extraídos) a ser rastreados. Se o rastreamento for encerrado prematuramente por causa desse limite, o arquivo compactado permanecerá sem verificação.

Se desejar desativar o rastreamento de pastas controladas pelo sistema (*/proc* e */sys*), selecione a opção **Excluir pastas de controle do sistema do rastreamento**. (Essa opção não está disponível para rastreamento de inicialização.)

4.1.3.6 Outros

Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. A Otimização inteligente não é definida rigidamente no produto. A Equipe de desenvolvimento da ESET está implementando continuamente as novas alterações que foram integradas ao ESET NOD32 Antivirus por meio de atualizações regulares. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Rastrear fluxos dados alternativos (somente scanner sob demanda)
Fluxos de dados alternativos usados pelo sistema de arquivos são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Manter último registro de acesso (somente scanner sob demanda)
Marque essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (ou seja, para uso com sistemas de backup de dados).

4.1.4 Uma infiltração foi detectada

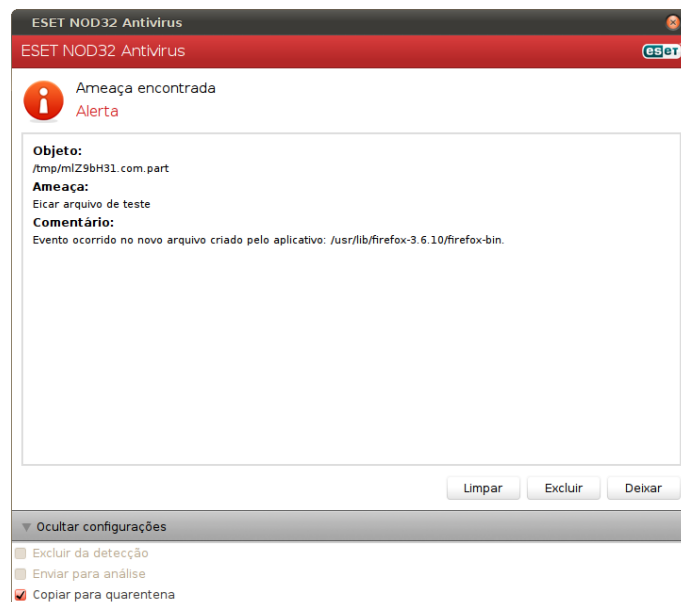
As infiltrações podem atingir o sistema a partir de vários pontos de entrada: páginas da Web, pastas compartilhadas, email ou dispositivos de computador removíveis (USB, discos externos, CDs, DVDs, disquetes etc.).

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência etc., recomendamos as seguintes etapas:

1. Abra o ESET NOD32 Antivirus e clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** (para obter mais informações, consulte a seção Rastreamento inteligente 12).
3. Após a conclusão do rastreamento, revise o relatório para obter informações como o número de arquivos rastreados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas no ESET NOD32 Antivirus, suponha que uma infiltração seja detectada pelo monitor do sistema de arquivos em tempo real, que usa o nível de limpeza padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida a ser tomada para o módulo de proteção em tempo real, você será solicitado a selecionar uma opção em uma janela de alertas. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. A seleção da opção **Nenhuma ação** não é recomendada, visto que os arquivos infectados são mantidos intocados. Uma exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

Limpeza e exclusão – Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou a esse arquivo um código malicioso. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Exclusão de arquivos em arquivos compactados - No modo de limpeza padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Entretanto, tome cuidado ao realizar um rastreamento de **Limpeza rígida**. Com esse tipo de limpeza, o arquivo será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

4.2 Atualização do programa

As atualizações regulares do ESET NOD32 Antivirus são necessárias para manter o nível máximo de segurança. O módulo de atualização ajuda a garantir que o sistema esteja sempre atualizado por meio da atualização do banco de dados de assinatura de vírus.

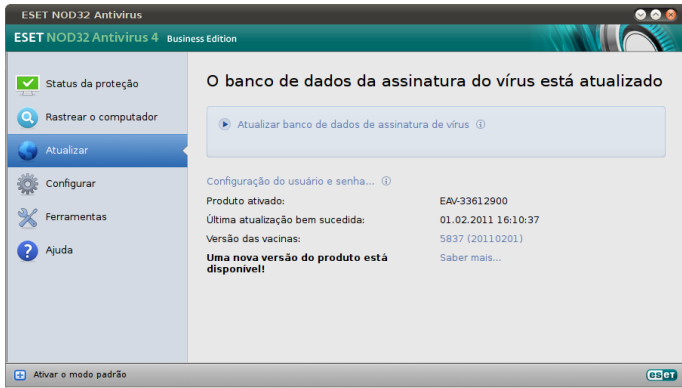
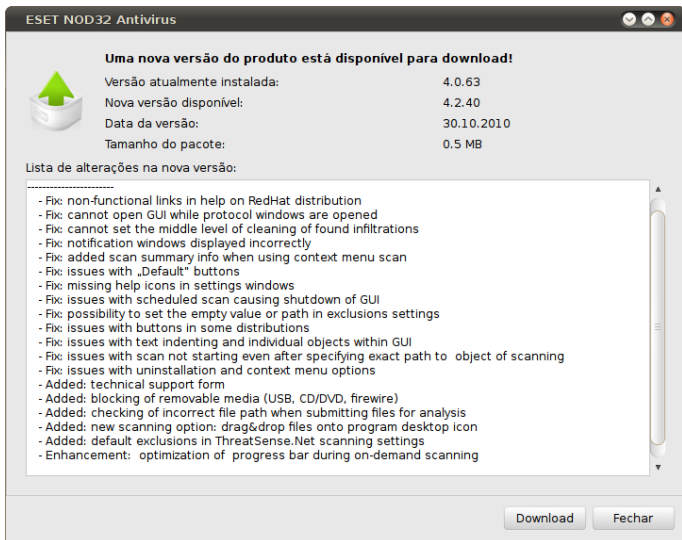
No menu principal, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. Para iniciar o processo de atualização manualmente, clique em **Atualizar banco de dados de assinatura de vírus**.

Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **O banco de dados de assinatura de vírus está atualizado** aparecerá na janela Atualizar. Se o banco de dados de assinatura de vírus não puder ser atualizado, recomendamos que você verifique as configurações de atualização 16. O motivo mais comum para esse erro são dados de autenticação digitados incorretamente (Usuário e Senha), ou configurações de conexão 22 incorretas.

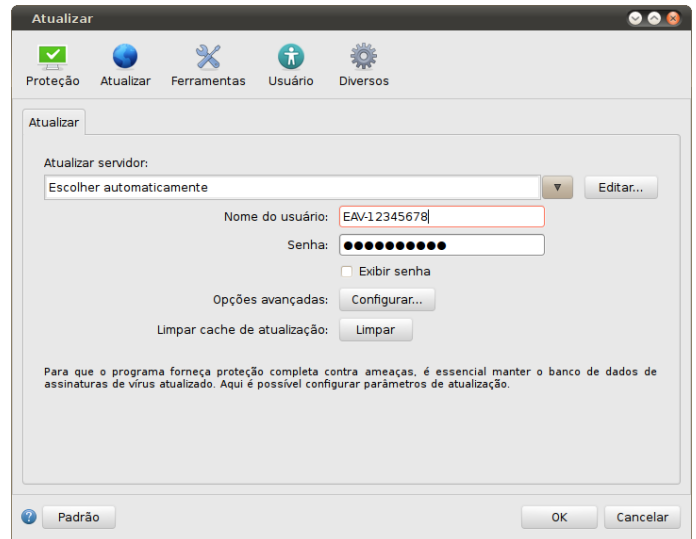
A janela Atualizar também contém informações sobre a versão o banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas durante determinada atualização.

OBSERVAÇÃO: O seu usuário e a sua senha são fornecidos pela ESET após a compra do ESET NOD32 Antivirus.

4.2.1 Atualização para uma nova compilação

Para obter a máxima proteção, é importante usar a compilação mais recente do ESET NOD32 Antivirus. Para verificar se há uma nova versão, clique em **Atualizar** no menu principal à esquerda. Se uma nova compilação estiver disponível, uma mensagem que informa *Uma nova versão do produto está disponível!* será exibida na parte inferior da janela. Clique em **Saber mais...** para exibir uma nova janela que contenha o número da versão da nova compilação e o log de alterações.

Clique em **Download** para fazer download da compilação mais recente. Clique em **Fechar** para fechar a janela e fazer download da atualização mais tarde.

Se você clicou em **Download**, o arquivo será obtido por download para a sua pasta de downloads (ou para a pasta padrão definida pelo navegador). Quando o download do arquivo estiver concluído, inicie o arquivo e siga as instruções de instalação. O seu nome de usuário e a sua senha serão automaticamente transferidos para a nova instalação. É recomendável verificar se há atualizações regularmente, especialmente quando instalar o ESET NOD32 Antivirus usando CD/DVD.

4.2.2 Configuração da atualização

A seção de configuração da atualização especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede.

A lista de servidores de atualização disponíveis pode ser acessada por meio do menu suspenso **Servidor de atualização** . Para adicionar um novo servidor de atualização, clique em **Editar...** Insira o endereço do novo servidor no campo de entrada **Servidor de atualização** e clique no botão **Adicionar**. A autenticação dos servidores de atualização é baseada no **Usuário** e na **Senha** gerados e enviados a você após a compra.

Para ativar a utilização do modo de teste (modo de teste de downloads), clique no botão **Configurar...** ao lado de **Opções avançadas** e marque a caixa de seleção **Ativar modo de teste**. Para desativar as notificações da bandeja do sistema que são exibidas após cada atualização bem-sucedida, marque a caixa de seleção **Não exibir notificação sobre atualização bem-sucedida**.

Para excluir todos os dados de atualização armazenados temporariamente, clique no botão **Limpar** ao lado de **Limpar cache de atualização**. Utilize essa opção se estiver com dificuldades durante a atualização.

4.2.3 Como criar tarefas de atualização

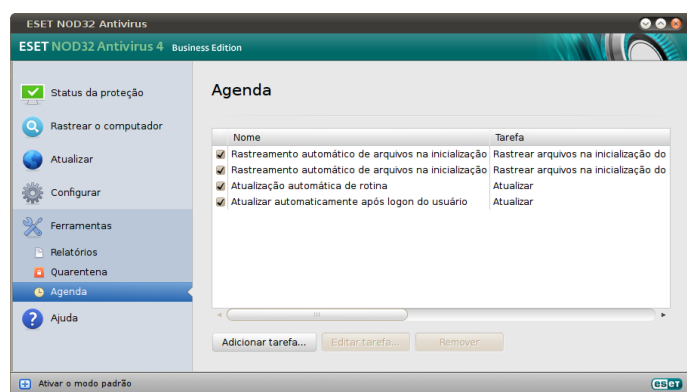
As atualizações podem ser disparadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela primária, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET NOD32 Antivirus:

- **Atualização automática de rotina**
- **Atualizar automaticamente após logon do usuário**

Cada uma das tarefas de atualização mencionadas pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda 17.

4.3 Agenda

A **Agenda** ficará disponível se o Modo avançado no ESET NOD32 Antivirus estiver ativado. A Agenda pode ser encontrada no menu principal do ESET NOD32 Antivirus em **Ferramentas**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

Por padrão, as seguintes tarefas agendadas são exibidas na Agenda:

- Atualização automática de rotina
- Atualizar automaticamente após logon do usuário
- Rastreamento de arquivos em execução durante inicialização do sistema após logon do usuário
- Rastreamento de arquivos em execução durante inicialização do sistema após atualização bem sucedida do banco de dados de assinatura de vírus
- Manutenção de relatórios (após a ativação da opção **Mostras as tarefas do sistema** na configuração da agenda)

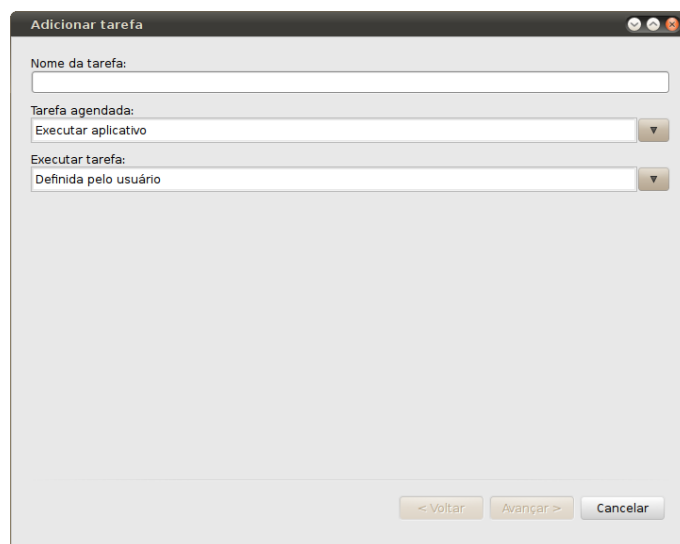
Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

4.3.1 Finalidade do agendamento de tarefas

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

4.3.2 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar tarefa...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo**
- **Atualizar**
- **Manutenção de relatórios**
- **Rastreamento sob demanda do computador**
- **Rastrear arquivos na inicialização do sistema**

Como Atualizar é uma das tarefas agendadas usadas com mais frequência, nós explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Digite o nome da tarefa no campo **Nome da tarefa**. Selecione a frequência da tarefa no menu suspenso **Executar tarefa**. As opções disponíveis são: **Definida pelo usuário**, **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento disparado**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a caixa de rolagem **Intervalo mínimo da tarefa**)

Na próxima etapa, uma janela de resumo com as informações sobre a tarefa agendada atual será exibida. Clique no botão **Finalizar**.

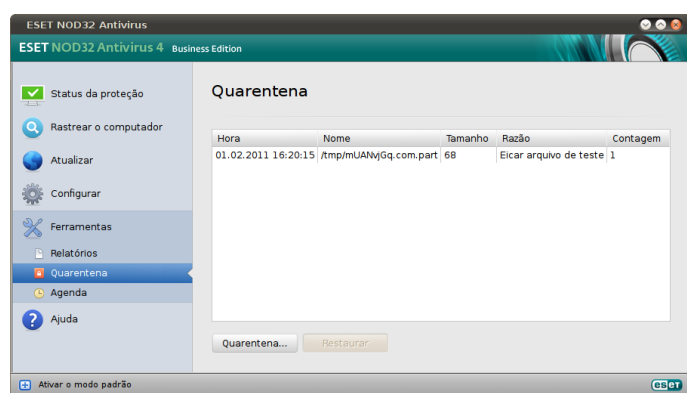
A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

O sistema, por padrão, contém as tarefas agendadas necessárias para garantir a funcionalidade correta do produto. Elas não devem ser alteradas e ficam ocultas, por padrão. Para

alterar essa opção e tornar essas tarefas visíveis, entre em **Configuração** > **Entrar nas preferências do aplicativo ...** > **Ferramentas** > **Agenda** e selecione a opção **Mostrar tarefas do sistema**.

4.4 Quarentena

A principal tarefa da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET NOD32 Antivirus.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo scanner antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de ameaças da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e o horário da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, adicionado pelo usuário...) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças). A pasta de quarentena com os arquivos em quarentena (*/var/opt/eset/esets/cache/quarantine*) permanecerá no sistema mesmo após a desinstalação do ESET NOD32 Antivirus. Os arquivos em quarentena são armazenados em um formato criptografado e seguro e podem ser restaurados novamente após a instalação do ESET NOD32 Antivirus.

Se desejar rastrear automaticamente arquivos em quarentena depois de cada atualização do banco de dados da assinatura de vírus, selecione a opção **Rastrear novamente arquivos em quarentena após cada atualização** em **Configuração** > **Entrar nas preferências do aplicativo...** > **Ferramentas** > **Quarentena** .

4.4.1 Colocação de arquivos em quarentena

O ESET NOD32 Antivirus coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Quarentena...**. O menu de contexto pode ser utilizado também para essa finalidade; clique com o botão direito do mouse na janela **Quarentena**, escolha o arquivo que deseja colocar em quarentena e clique no botão **Abrir**.

4.4.2 Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Utilize o botão **Restaurar** para essa finalidade. O botão Restaurar também está disponível no menu de contextos, clicando com o botão direito do mouse no arquivo determinado, na janela **Quarentena**, e, em seguida, clicando em **Restaurar**. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

4.4.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de ameças da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar arquivo para análise** no menu de contexto.

4.5 Relatórios

Os Relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas. Os Relatórios atuam como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. Os Relatórios são realizados ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do relatório. É possível visualizar mensagens de texto e relatórios diretamente do ambiente do ESET NOD32 Antivirus, bem como arquivar relatórios.

Os relatórios podem ser acessados no menu principal do ESET NOD32 Antivirus, clicando em **Ferramentas** > **Relatórios**. Selecione o tipo de relatório desejado, utilizando o menu suspenso **Relatório** da parte superior da janela. Os seguintes relatórios estão disponíveis:

1. **Ameaças detectadas** – Use essa opção para exibir todas as informações sobre eventos relacionados à detecção de infiltrações.
2. **Eventos** - Essa opção foi desenvolvida para a solução de problemas de administradores do sistema e usuários. Todas as ações importantes executadas pelo ESET NOD32 Antivirus são registradas nos Relatórios de eventos.
3. **Rastrear o computador** - Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo Rastreamento sob demanda do computador.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar**.

4.5.1 Manutenção de relatórios

A configuração de relatórios do ESET NOD32 Antivirus pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar nas preferências do aplicativo ...** > **Ferramentas** > **Relatórios**. Você pode especificar as seguintes opções para relatórios:

- **Excluir relatórios antigos automaticamente** - as entradas de relatórios anteriores ao número de dias especificado são automaticamente excluídas.
- **Otimizar automaticamente relatórios** - ativa a desfragmentação automática de relatórios se a porcentagem especificada de relatórios não utilizados foi excedida.

Para configurar o **Filtro padrão dos relatórios**, clique no botão **Editar...** e marque/desmarque os tipos de relatórios, conforme a necessidade.

4.5.2 Filtragem de relatórios

Registra em relatório as informações de armazenamento sobre eventos importantes do sistema: O recurso de filtragem de relatórios permite exibir registros sobre um tipo específico de evento.

Os tipos de relatórios utilizados com mais frequência são listados a seguir:

- **Avisos críticos** - erros críticos do sistema (por exemplo, falha em iniciar a proteção antivírus)
- **Erros** - mensagens de erro, como "*Erro ao fazer download de arquivo*" e erros críticos
- **Avisos** - mensagens de avisos
- **Registros informativos** - mensagens informativas, incluindo atualizações bem sucedidas, alertas etc.
- **Registros de diagnóstico** - informações necessárias para ajustar o programa e também todos os registros descritos acima.
- **Todos os filtros** - utilize essa caixa de seleção para marcar/desmarcar todos os tipos de relatórios relacionados acima.

4.6 Interface do usuário

As opções de configuração da interface do usuário no ESET NOD32 Antivirus permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas configurações podem ser acessadas em **Configuração** > **Entrar nas preferências do aplicativo ...** > **Usuário** > **Interface**.

Nessa seção, a opção Modo avançado proporciona aos usuários a capacidade de permitir a alternância para o Modo avançado. O Modo avançado exibe as configurações mais detalhadas e os controles adicionais do ESET NOD32 Antivirus.

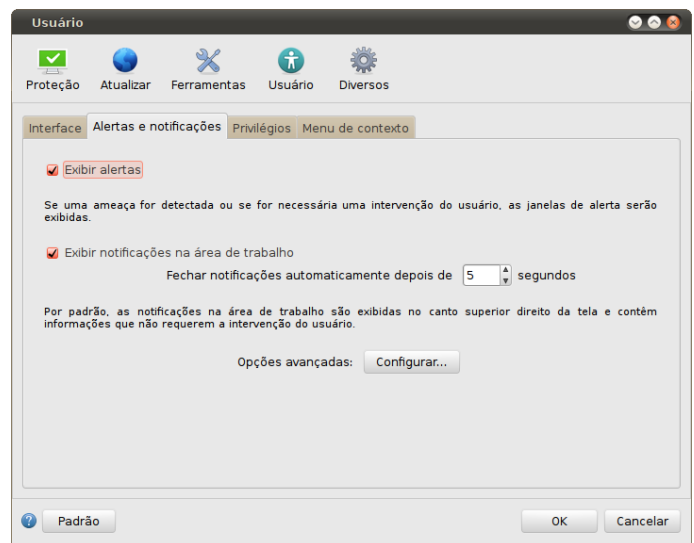
Para ativar a funcionalidade de tela inicial na inicialização, selecione a opção **Mostrar tela inicial na inicialização**.

Na seção **Usar menu padrão**, você pode selecionar as opções **No modo padrão/No modo avançado** para ativar a utilização do menu padrão na janela principal do programa no(s) respectivo(s) modo(s) de exibição.

Para ativar a utilização das dicas de ferramenta, selecione a opção **Mostrar dicas de ferramentas**. A opção **Mostrar arquivos ocultos** permite que você veja e selecione arquivos ocultos na configuração **Alvos de rastreamento** de um **Rastrear o computador**.

4.6.1 Alertas e notificações

A seção **Alertas e notificações** permite que você configure a maneira como os alertas de ameaças e as notificações do sistema são tratados no ESET NOD32 Antivirus.

A desativação da opção **Exibir alertas** cancelará todas as janelas de alertas e será adequada somente para situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

A seleção da opção **Exibir notificações na área de trabalho** ativará as janelas de alertas que não exigem a interação do usuário para serem exibidas na área de trabalho (por padrão, no canto superior direito da sua tela). Você pode definir o período no qual a notificação será exibida, ajustando o valor de **Fechar notificações automaticamente depois de** X **segundos**.

4.6.1.1 Configuração avançada de alertas e notificações

Exibir somente notificações que requerem interação do usuário
Com essa opção, você pode alternar a exibição das mensagens que exijam a interação do usuário.

Exibir somente notificações que requerem interação do usuário ao executar aplicativos em modo de tela inteira
Essa opção é útil durante apresentações, jogos ou outras atividades que exijam o modo de tela cheia.

4.6.2 Privilégios

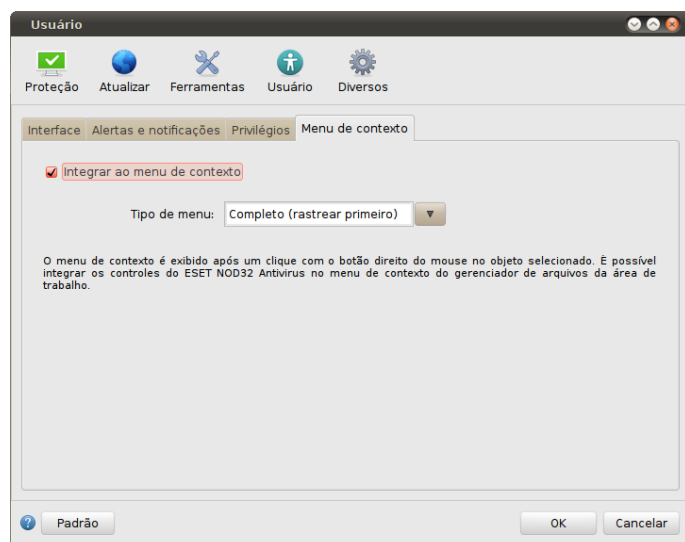
As configurações do ESET NOD32 Antivirus podem ser muito importantes para a política de segurança da organização. Modificações não autorizadas podem pôr em risco a estabilidade e a proteção do seu sistema. Consequentemente, você pode escolher quais usuários terão permissão para editar a configuração do programa.

Para especificar os usuários privilegiados, acesse **Configuração** > **Entrar nas preferências do aplicativo ...** > **Usuário** > **Privilégios**.

Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma lista de usuários privilegiados, basta selecioná-los na lista **Usuários** do lado esquerdo e clicar no botão **Adicionar**. Para remover um usuário, basta selecionar o nome dele/dela na lista **Usuários privilegiados** do lado direito e clicar em **Remover**.

OBSERVAÇÃO: Se a lista de usuários privilegiados estiver vazia, todos os usuários do sistema terão permissão para editar as configurações do programa.

4.6.3 Menu de contexto

A integração do menu de contexto pode ser ativada na seção **Configuração** > **Entrar nas preferências do aplicativo ...** > **Usuário** > **Menu de contexto**, marcando-se a caixa de seleção **Integrar ao menu de contexto**.

OBSERVAÇÃO: Para ativar a integração do menu de contexto, verifique se a extensão nautilius-actions está instalada.

4.7 ThreatSense.Net

O ThreatSense.Net Early Warning System mantém a ESET contínua e imediatamente informada sobre novas infiltrações. O ThreatSense.Net Early Warning System bidirecional tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que vemos novas ameaças assim que elas aparecerem é fazermos "link" com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

1. Você pode decidir não ativar o ThreatSense.Net Early Warning System. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.
2. Você pode configurar o ThreatSense.Net Early Warning System para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado à ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar seu banco de dados de ameaças e a aprimorar a capacidade de detecção de ameaças do programa.

O ThreatSense.Net Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no seu computador e as informações sobre o sistema operacional do seu computador.

Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador (usuários em um caminho de diretório etc.) para o nosso Laboratório de ameaças da ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

A configuração do ThreatSense.Net pode ser acessada na janela Configuração avançada, em **Ferramentas** > **ThreatSense.Net**. Selecione a opção **Ativar o ThreatSense.Net Early Warning System** para ativá-lo e clique no botão **Configurar...** ao lado do título Opções avançadas.

4.7.1 Arquivos suspeitos

A opção Arquivos suspeitos permite configurar a maneira como as ameaças serão enviadas ao Laboratório de ameaças da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo ao nossos Laboratórios de ameaças para análise. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização do banco de dados de assinatura de vírus.

Envio de arquivos suspeitos - Você pode optar por enviar esses arquivos **Durante a atualização**, ou seja, eles serão enviados ao Laboratório de ameaças da ESET durante uma atualização normal do banco de dados de assinatura de vírus. Como alternativa, você pode optar por enviá-los **O mais breve possível** - essa configuração será adequada se uma conexão permanente com a Internet estiver disponível.

Se não desejar que os arquivos sejam enviados, selecione a opção **Não enviar**. A seleção da opção de não envio de arquivos para análise não influencia no envio das informações estatísticas, pois elas são configuradas em uma área separada.

O ThreatSense.Net Early Warning System coletará informações anônimas sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. As estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

Abaixo, veja o exemplo de um pacote estatístico enviado:

```
# utc_time=2009-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=2.6.18-128.e5
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=/home/user/Documents/Incoming/rdgFR1463
[1].zip
```

Envio de informações estatísticas anônimas - Você pode definir o momento em que as informações estatísticas serão enviadas. Se optar por enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Esta configuração é adequada se uma conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, todas as informações estatísticas serão enviadas durante a atualização após a coleta.

Se não desejar enviar informações estatísticas anônimas, você poderá selecionar a opção **Não enviar**.

Distribuição de envio - Você pode selecionar como os arquivos e as informações estatísticas serão enviados à ESET. Selecione a opção **Remote Administrator Server ou ESET** para arquivos e estatísticas que serão enviados por qualquer meio disponível. Selecione a opção **Remote Administrator Server** para enviar os arquivos e as estatísticas ao servidor de administração remota, que, em seguida, os enviará ao Laboratório de ameaças da ESET. Se a opção **ESET** estiver selecionada, todos os arquivos suspeitos e informações estatísticas serão enviados ao laboratório de vírus da ESET diretamente do programa.

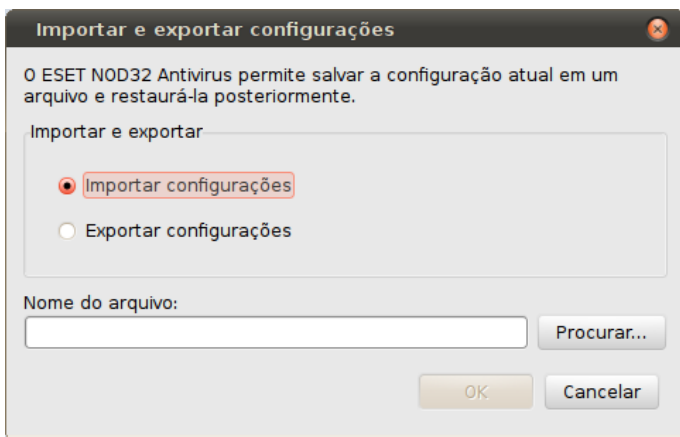
Filtro de exclusões - Essa opção permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (*.doc*, etc.). Você pode adicionar os tipos de arquivos à lista de arquivos excluídos.

Email de contato (opcional) - Seu email pode ser enviado com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

5. Usuário avançado

5.1 Importar e exportar configurações

A importação e a exportação das configurações do ESET NOD32 Antivirus estão disponíveis no modo Avançado, em **Configuração**.

A Importação e a Exportação utilizam arquivos compactados para armazenar a configuração. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET NOD32 Antivirus para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET NOD32 Antivirus em diversos sistemas. Os usuários também podem importar o arquivo de configuração para transferir as configurações desejadas.

5.1.1 Importar configurações

A importação de uma configuração é muito fácil. No menu principal, clique em **Configuração** > **Importar e exportar configurações ...** e selecione a opção **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão **Procurar...** para procurar o arquivo de configuração que deseja importar.

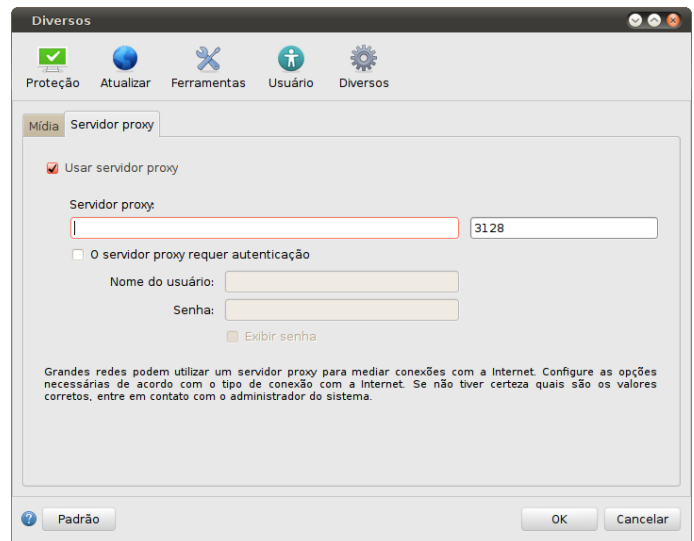
5.1.2 Exportar configurações

As etapas para exportar uma configuração são muito semelhantes. No menu principal, clique em **Configuração** > **Importar e exportar configurações ...** Selecione a opção **Exportar configurações** e digite o nome do arquivo de configuração. Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

5.2 Configuração do servidor proxy

As configurações do servidor proxy podem ser definidas em **Diversos** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET NOD32 Antivirus. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da porta do servidor proxy.

Se a comunicação com o servidor proxy requer autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos.

5.3 Bloqueio de mídia removível

Mídias removíveis (por exemplo, CD ou chave USB) podem conter código malicioso e colocar o computador em risco. Para bloquear a mídia removível, marque a opção **Ativar bloqueio de mídia removível**. Para permitir o acesso a determinados tipos de mídia, desmarque os volumes de mídia desejados.

5.4 Administração remota

O ESET Remote Administrator (ERA) é uma ferramenta utilizada para gerenciar a política de segurança e para obter uma visão geral de toda a segurança em uma rede. É especialmente útil quando aplicada a redes maiores. O ERA não aumenta somente o nível de segurança mas também fornece facilidade de uso, gerenciando o ESET NOD32 Antivirus em estações de trabalho cliente.

As opções de configuração de administração remota estão disponíveis na janela principal do programa ESET NOD32 Antivirus. Clique em **Configuração > Entrar nas preferências do aplicativo ... > Diversos > Administração remota**.

Ative a administração remota selecionando a opção **Conectar ao servidor de Administração Remota**. É possível acessar as opções descritas a seguir:

Intervalo de conexões do servidor - Essa opção designa a frequência com que o ESET NOD32 Antivirus conectará ao ERA Server. Se estiver configurada como **0**, as informações serão enviadas a cada 5 segundos.

Remote Administrator Server - Endereço de rede do servidor (onde o ERA Server é instalado) e o número da porta. Esse campo contém uma porta de servidor predefinida, que é utilizada para a conexão de rede. Recomendamos que você deixe a configuração de porta padrão em *2222*.

O servidor do Remote Administrator requer autenticação - Senha para a conexão com o ERA Server, se necessário.

Normalmente, somente o servidor **Primário** precisa ser configurado. Se estiver executando diversos servidores ERA na rede, é possível optar por adicionar outra conexão do ERA Server **Secundário**. Servirá como a solução de fallback. Se o servidor primário ficar inacessível, o ESET NOD32 Antivirus entrará em contato automaticamente com o ERA Server secundário. O ESET NOD32 Antivirus também tentará restabelecer a conexão com o servidor primário. Depois que essa conexão estiver ativa novamente, o ESET NOD32 Antivirus retornará ao servidor primário. A configuração de dois perfis de servidores de administração remota é mais bem utilizada por clientes móveis com notebooks que se conectam à rede local e fora da rede.

6. Glossário

6.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

6.1.1 Vírus

Um vírus de computador é uma infiltração que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente arquivos, scripts e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução do arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que um usuário (acidental ou deliberadamente) execute ou abra o programa malicioso.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus (quando comparados a cavalos de troia ou spyware) estão se tornando cada vez mais raros, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é frequentemente usado de maneira incorreta para cobrir todos os tipos de infiltrações. Essa utilização está gradualmente sendo superada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

Os exemplos de vírus são: *OneHalf*, *Tenga* e *Yankee Doodle*.

6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms são propagados por meio dos endereços de e-mail da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas após sua liberação – em alguns casos, até em minutos. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* e *Netsky*.

6.1.3 Cavalos de troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de infiltrações que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Hoje não há mais a necessidade de cavalos de troia para que eles se disfarcem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "Cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- Downloader – Um programa malicioso com a capacidade de fazer o download de outras infiltrações da Internet.
- Dropper – Um tipo de cavalo de troia projetado para instalar outros tipos de malware em computadores comprometidos.
- Backdoor – Um aplicativo que se comunica com agressores remotos, permitindo que eles obtenham acesso a um sistema e assumam o controle dele.
- Keylogger – (keystroke logger) – Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- Dialer – Dialers são programas projetados para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.
- Os cavalos de troia geralmente tomam a forma de arquivos executáveis. Se um arquivo em seu computador for detectado como um cavalo de troia, recomendamos excluí-lo, uma vez que é muito provável que ele contenha códigos maliciosos.

Os exemplos dos cavalos de troia bem conhecidos são: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

6.1.4 Adware

Adware é a abreviação de advertising-supported software (software suportado por propaganda). Os programas que exibem material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage do mesmo. O

adware é frequentemente vinculado a programas freeware, permitindo que os desenvolvedores de programas freeware cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O adware por si só não é perigoso; os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware também pode realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Os programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

6.1.5 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de e-mail da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias. etc. O spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor, a fim de gerar lucro ou de oferecer um incentivo para a compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, nós recomendamos excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

6.1.6 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET NOD32 Antivirus fornece a opção de detectar tais ameaças.

"Aplicativos potencialmente inseguros" é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo inseguro em potencial presente e sendo executado em seu computador (e que você não instalou), consulte o seu administrador de rede ou remova o aplicativo.

6.1.7 Aplicativos potencialmente indesejados

Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o sistema se comportará de modo diferente (em comparação ao modo anterior à instalação desses aplicativos). As alterações mais significativas são:

- são abertas novas janelas que você não via anteriormente
- ativação e execução de processos ocultos
- uso aumentado de recursos do sistema
- alterações nos resultados de pesquisa
- o aplicativo se comunica com servidores remotos.